

On the Achievable Error Region of Physical Layer Authentication Techniques over Rayleigh Fading Channels

Augusto Ferrante*, Nicola Laurenti*, Chiara Masiero*, Michele Pavon[†], and

Stefano Tomasin*

* Department of Information Engineering, University of Padova, Italy

[†] Department of Mathematics, University of Padova, Italy

Email: {first_name.last_name}@dei.unipd.it

Abstract

For a physical layer message authentication procedure based on the comparison of channel estimates obtained from the received messages, we focus on an outer bound on the type I/II error probability region. Channel estimates are modelled as multivariate Gaussian vectors, and we assume that the attacker has only some side information on the channel estimate, which he does not know directly. We derive the attacking strategy that provides the tightest bound on the error region, given the statistics of the side information. This turns out to be a zero mean, circularly symmetric Gaussian density whose correlation matrices may be obtained by solving a constrained optimization problem. We propose an iterative algorithm for its solution: Starting from the closed form solution of a relaxed problem, we obtain, by projection, an initial feasible solution; then, by an iterative procedure, we look for the fixed point solution of the problem. Numerical results show that for cases of interest the iterative approach converges, and perturbation analysis shows that the found solution is a local minimum.

Index Terms

Authentication, Physical layer security, Rayleigh fading channels, Hypothesis testing

I. INTRODUCTION

Physical layer security provides an effective defense mechanism which is complementary to higher layer security techniques. Indeed, it has the potential of resisting the attacks based on computational capabilities that may be feasible in the near future, e.g., by quantum computing.

Moreover, security implemented at the physical layer is usually based on information theoretic arguments. It therefore entails analytically predictable performance irrespective of the attacker capabilities. One of the most desirable mechanisms of physical layer security is the authentication of the message source. This key task can be conveniently recast into a hypothesis testing problem [9], [14], namely to decide between hypothesis \mathcal{H}_0 that the message was effectively sent by the legitimate source, and hypothesis \mathcal{H}_1 that it was forged by the attacker.

Physical layer authentication has been addressed by considering either device-specific non-ideal transmission parameters extracted from the received signal [2], or channel characteristics to identify the link between a specific source and the receiver [5], [7], [8]. In this paper we focus on the latter case, which finds application in many wideband wireless systems, where even small changes in the position of the transmitter have a significant impact on the channel. In particular, we consider the approach of [8], where the test is performed in two phases. In the first phase, the receiver gets an authenticated noisy estimate x of the channel with respect to the legitimate transmitter. In the second phase, upon reception of a message, the receiver gets a new estimate u of the channel and compares it with x . Then, he must decide whether u is an estimate of the legitimate channel or the channel forged by an eavesdropper.

The performance of a binary hypothesis testing scheme is measured by the probability of type I (false alarm), and type II (missed detection) errors. Therefore, theoretical bounds on the achievable error probability region are of great importance to establish the effectiveness of practical schemes. For instance, [9] considered the traditional authentication scenario in which the legitimate parties can make use of a shared cryptographic key that is kept perfectly secret to the attackers. There, an outer bound on the achievable error region was derived, that holds irrespectively of the decision rule implemented by the receiver. Then, by fixing the false alarm probability, the outer bound is turned into a lower bound on the missed detection probability. An analogous approach was used in [11] and [13] within the different contexts of steganography and fingerprinting, respectively. Similarly, in [14], such lower bound is paired with an asymptotic upper bound, and both are derived also in the case that the legitimate parties share correlated sequences, instead of an identical key.

In the above cases, since the attacker has no information on the shared sequences, the optimal attack strategy with respect to the outer bound is to present forged signals that, albeit independent of the legitimate shared key, are generated from the same marginal distribution as the legitimate

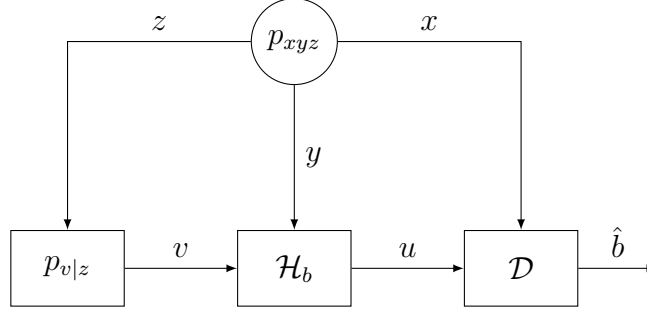


Fig. 1: Abstract model for physical layer authentication cast as an hypothesis testing problem with channel estimates as the available observations.

signals. In our framework, on the contrary, the legitimate authentication signal is the actual realization of a fading wireless channel. Thus the attacker has some side information given by the channel estimates z he performs, which are in general correlated with the legitimate channel. We model channel estimates as correlated multivariate Gaussian vectors, which is a usual assumption in wireless transmissions, including those using orthogonal frequency division multiplexing (OFDM) or multi-antenna (multiple input multiple output, MIMO).

The contribution of our paper is thus threefold: 1) we derive an outer bound to the error probability region, in terms of the attacker strategy; 2) we prove the existence of a strategy v , jointly Gaussian with z , that yields the tightest bound, and characterize the covariance through the solution of a system of two matrix equations; 3) we give an efficient technique for the numerical evaluation of the optimal attack strategy and the corresponding bound.

The paper is organized as follows. Section II introduces the problem formally, so that the theoretical results can be derived in Section III. Based on those results, in Section IV we propose an efficient algorithm for the numerical evaluation of the optimal attack strategy. Then, in Section V we give examples of numerical results, and eventually we draw conclusions in Section VI.

In our notation, if $a \in \mathcal{C}^n$ and $b \in \mathcal{C}^m$ are random vectors, K_{ab} denotes the $n \times m$ covariance matrix of vectors a and b , whereas $K \begin{bmatrix} a \\ b \end{bmatrix}$ stands for the $(n+m) \times (n+m)$ variance matrix of the vector $\begin{bmatrix} a \\ b \end{bmatrix}$. The symbol A^* denotes the complex conjugate transpose of matrix A .

II. PROBLEM STATEMENT

We consider the physical layer channel authentication scheme where agents Alice and Eve transmit messages to Bob, and Bob aims at authenticating messages from Alice, i.e., deciding whether she sent them or not. The authentication is performed via a two phase procedure, as detailed in [8]:

a) First Phase: In the first phase Alice transmits one or more messages, whose authenticity is guaranteed by higher layer techniques. Bob gets a noisy estimate x of the channel with respect to Alice and replies with acknowledge messages. Moreover, upon Alice and Bob transmissions, Eve gets (possibly noisy) estimates of her own channel with respect to both the other agents: the set of these two estimates is denoted with z .

b) Second Phase: In the second phase, either Alice or Eve transmits messages. Bob authenticates the received messages by getting a new noisy channel estimate u and comparing it with his template x . If this decision process \mathcal{D} deems the message as coming from Alice, the binary flag \hat{b} is set to zero, otherwise it is set to one. In this phase, Alice performs transmissions in the same fashion of the first phase, while Eve performs a pre-processing of her own messages in order to induce an equivalent channel estimate by Bob that is as close as possible to x .

An abstract representation of the authentication scenario is given in Fig. 1. We assume that Eve is able to forge any equivalent channel v to Bob, through a probabilistic strategy, based on her observations z , which can be characterized by the conditional distribution $p_{v|z}$. Although constraints on power and channel characteristics may in practice prevent this, the assumption is a worst case scenario, which is of interest to derive performance bounds. On the other hand, estimates of Alice-Bob channel in both the first and the second phase are not identical, in general, due to independent noise that affects both estimates. Let y denote a realization of the random channel estimate of the Alice-Bob channel. Given the channel estimate u , Bob decides between the two hypotheses

$$\mathcal{H}_0 : u = y \quad \text{message is from Alice ,} \quad (1)$$

$$\mathcal{H}_1 : u = v \quad \text{message was forged.} \quad (2)$$

In Fig. 1, being in hypothesis \mathcal{H}_0 or \mathcal{H}_1 is obtained by setting $b = 0$ or 1 , respectively. Correct authentication is achieved when $\hat{b} = b$.

Recall that all channels are described by zero-mean circular symmetric complex Gaussian vectors with correlated entries, as a suitable model for many scenarios (including MIMO/OFDM). Moreover, we assume that all transmissions are corrupted by additive white Gaussian noise with zero mean. Therefore, also the channel estimates are zero-mean circular symmetric complex Gaussian vectors with correlated entries. In particular, x , and y are n -dimensional, complex, circular symmetric Gaussian random vectors, z is an m -dimensional, complex, circular symmetric Gaussian random vector, while v is an n -dimensional, complex, random vector whose probability density is not specified as it will be chosen by the attacker in order to obtain better mimetic features. We denote the set of all possible conditional distributions (forging strategies) $p_{v|z}(\cdot|\cdot)$ as

$$\mathcal{Q} = \left\{ q(\cdot|\cdot) : \mathcal{C}^n \times \mathcal{C}^m \rightarrow \mathcal{R}, q(b|c) \geq 0, \int q(b|c) db = 1 \right\}. \quad (3)$$

Performance of the authentication system are assessed by type I error probability α , i.e., the probability that Bob discards a message as forged by Eve while it is coming from Alice

$$\alpha = \mathbb{P}[\hat{b} = 1 | \mathcal{H}_0], \quad (4)$$

and the type II error probability β , i.e., the probability that Bob accepts a message coming from Eve as legitimate

$$\beta = \mathbb{P}[\hat{b} = 0 | \mathcal{H}_1]. \quad (5)$$

The aim of a clever design for the authentication scheme is to make both error probabilities α and β as small as possible. Since it is trivial to achieve $\alpha + \beta = 1$ with a random decision strategy that outputs $\hat{b} = 1$ with probability α , independently of the observation u , we are only interested in values of α, β in the region

$$\mathcal{R}^0 = \{(\alpha, \beta) : \alpha \geq 0, \beta \geq 0, \alpha + \beta \leq 1\}. \quad (6)$$

A. Error Region Bounds for a Given Attacking Strategy

A first bound on the error region for a given attacking strategy can be obtained by applying the fundamental data processing inequality for the Kullback-Leibler (KL) divergence [12] to our binary hypothesis decision scheme \mathcal{D} . In fact, from [11], [9] we have¹

$$\mathcal{D}(p_{\hat{b}|\mathcal{H}_1} || p_{\hat{b}|\mathcal{H}_0}) \leq \mathcal{D}(p_{xu|\mathcal{H}_1} || p_{xu|\mathcal{H}_0}). \quad (7)$$

¹Note that the symmetric bound $\mathcal{D}(p_{\hat{b}|\mathcal{H}_0} || p_{\hat{b}|\mathcal{H}_1}) \leq \mathcal{D}(p_{xu|\mathcal{H}_0} || p_{xu|\mathcal{H}_1})$ also holds true (see also [8]).

First we observe that $p_{\hat{b}|\mathcal{H}_0}(1) = \alpha$, $p_{\hat{b}|\mathcal{H}_0}(0) = 1 - \alpha$, and similarly $p_{\hat{b}|\mathcal{H}_1}(0) = \beta$, $p_{\hat{b}|\mathcal{H}_1}(1) = 1 - \beta$. Therefore, introducing the function²

$$f(\varphi, \psi) = \varphi \log \frac{\varphi}{1 - \psi} + (1 - \varphi) \log \frac{1 - \varphi}{\psi}, \quad \varphi, \psi \in [0, 1] \quad (8)$$

we can rewrite (7) as

$$f(\beta, \alpha) \leq \mathcal{D}(p_{xu|\mathcal{H}_1} \| p_{xu|\mathcal{H}_0}) . \quad (9)$$

Since the observation z encloses all the information the attacker can exploit in order to deceive the receiver, we can assume that the forging strategy v is *conditional independent* of the secure template x , given z . Then the divergence on the right side of (9) can be written explicitly for a given attacking strategy $q(\cdot|\cdot) \in \mathcal{Q}$ as

$$D(q) = \mathcal{D}(p_{xu|\mathcal{H}_1} \| p_{xu|\mathcal{H}_0}) = \mathcal{D}(p_{xz} \| p_{xy}) \quad (10)$$

$$= \iint \left[\int p_{xz}(a, c) q(b|c) dc \right] \left[\log \left(\int p_{xz}(a, c) q(b|c) dc \right) - \log p_{xy}(a, b) \right] da db . \quad (11)$$

Let $f_0 \geq 0$ be given and set

$$\mathcal{R}(f_0) := \{(\alpha, \beta) \in \mathcal{R}^0 : f(\beta, \alpha) \leq f_0\} . \quad (12)$$

Then (9) can be rewritten as

$$(\alpha, \beta) \in \mathcal{R}(D(q)) . \quad (13)$$

B. Error Region Bounds for Any Attacking Strategy

Each outer bound in (13) is clearly looser than

$$\mathcal{R}_\cap = \bigcap_{q \in \mathcal{Q}} \mathcal{R}(D(q)) = \mathcal{R}(D^\star) \quad (14)$$

where

$$D^\star = \inf_{q \in \mathcal{Q}} D(q) . \quad (15)$$

²Notice that $f(\varphi, \psi)$ is the KL divergence between two Bernoulli probability distributions of parameters φ and $1 - \psi$, respectively.

Note that the region in (14) is not strictly speaking an outer bound of the type (13), since the infimum (15) may, in general, not be achievable. In that case, (14) represents a worst case performance for the authentication system, over all possible attacking strategies. On the other hand, for the attacker, approaching (15) represents the possibility to effectively carry out an impersonation attack.

The main goal of this paper is to evaluate the tightest bound (14). Indeed, we provide an attacking strategy achieving (15), under the assumption that the observation z encodes all the information about the secure template x the attacker can rely on in order to deceive the receiver. We have just shown that this is equivalent to the following constrained optimization problem:

Problem 1: Given the zero-mean, circular symmetric, jointly Gaussian random vectors x, y, z with joint covariance matrix

$$K \begin{bmatrix} x \\ y \\ z \end{bmatrix} := \begin{bmatrix} K_{xx} & K_{xy} & K_{xz} \\ K_{yx} & K_{yy} & K_{yz} \\ K_{zx} & K_{zy} & K_{zz} \end{bmatrix}, \quad (16)$$

find a joint probability distribution $p_{xvz} \in L^1(\mathbb{C}^{2n+m})$ such that its marginal p_{xv} minimizes $\mathcal{D}(p_{xv} || p_{xy})$ under the constraints:

1. The marginal distribution of x, z (corresponding to p_{xvz}) is equal to the given distribution p_{xz} .
2. The random vectors v and x are conditionally independent given z .

III. MAIN RESULTS

In this section, we address Problem 1. In particular, we show that the problem is feasible, that it admits an optimal solution and that this solution is Gaussian. Finally, we show how to reformulate this problem in terms of solutions of two coupled matrix equations. The first issue to be considered is the *feasibility* of Problem 1, namely the existence of a distribution p_{xvz} satisfying the constraints and such that $\mathcal{D}(p_{xv} || p_{xy})$ is finite.

Lemma 1: Problem 1 is feasible.

Proof: Let v be an n -dimensional, complex, zero-mean, circular symmetric Gaussian random vector (with arbitrary covariance) independent of x and of z . It is immediate to check that the corresponding p_{xvz} satisfies the constraints and is such that $\mathcal{D}(p_{xv} || p_{xy})$ is finite. ■

Lemma 2: Let x and z be jointly Gaussian. For any attacking strategy p_{xv} having finite second moment and in which v and x are conditionally independent given z , they are also conditionally

orthogonal given z , that is

$$\mathbb{E} [(x - \bar{\mathbb{E}}[x|z])(v - \bar{\mathbb{E}}[v|z])] = 0, \quad (17)$$

where $\bar{\mathbb{E}}[\cdot|z]$ stands for the best linear estimator of \cdot given z

Proof: We have

$$\mathbb{E} [(x - \bar{\mathbb{E}}[x|z])(v - \bar{\mathbb{E}}[v|z])] = \mathbb{E} [\mathbb{E} [(x - \bar{\mathbb{E}}[x|z])(v - \bar{\mathbb{E}}[v|z])|z]] \quad (18)$$

$$= \mathbb{E} [\mathbb{E} [(x - \bar{\mathbb{E}}[x|z])|z] \mathbb{E} [(v - \bar{\mathbb{E}}[v|z])|z]] \quad (19)$$

$$= \mathbb{E} [(\mathbb{E}[x|z] - \bar{\mathbb{E}}[x|z]) (\mathbb{E}[v|z] - \bar{\mathbb{E}}[v|z])] , \quad (20)$$

where (18) and (19) follow from the Total Expectation Theorem and the definition of conditional independence, respectively. Since x and z are jointly Gaussian, we have that $\mathbb{E}[x|z] = \bar{\mathbb{E}}[x|z]$. Thus, we can conclude that the right-hand side of (20) is equal to zero. ■

In general, conditional independence does not imply conditional orthogonality, although for jointly Gaussian variables they are equivalent. However, we have proved that conditional independence of x and v given z implies that x and v are conditionally orthogonal given z , thanks to x and z being jointly Gaussian.

Let us recall the joint covariance matrix (16)

$$K \begin{bmatrix} x \\ v \\ z \end{bmatrix} := \begin{bmatrix} K_{xx} & K_{xv} & K_{xz} \\ K_{vx} & K_{vv} & K_{vz} \\ K_{zx} & K_{zv} & K_{zz} \end{bmatrix}. \quad (21)$$

Notice that, since the attacker knows the joint probability density p_{xyz} , the corner elements of (21) are known. For the sake of simplicity, we introduce the following symbols for the unknown blocks of (21):

$$X := K_{vv}, \quad Y := K_{xv}, \quad Z := K_{vz}. \quad (22)$$

Hence, we can write

$$K \begin{bmatrix} x \\ v \\ z \end{bmatrix} = \begin{bmatrix} K_{xx} & Y & K_{xz} \\ Y^* & X & Z \\ K_{xz}^* & Z^* & K_{zz} \end{bmatrix}. \quad (23)$$

Recall that the conditional orthogonality of x and v given z is equivalent to the following zero-block pattern in its inverse³

$$K^{-1} \begin{bmatrix} x \\ v \\ z \end{bmatrix} = \begin{bmatrix} * & 0 & * \\ 0 & * & * \\ * & * & * \end{bmatrix}. \quad (24)$$

In this way we have expressed the second constraint of Problem 1 in terms of the structure of the inverse of the covariance matrix. We can therefore enforce this constraint by resorting to a “maximum entropy” completion as described in [3], see also [6] for a more general result and [1] for an application of this technique.

Lemma 3: If q_G is a circular symmetric Gaussian distribution, then, among all distributions p that share the same mean vector μ and covariance matrix K , the one that minimizes $\mathcal{D}(p \| q_G)$ is circular symmetric and Gaussian.

Proof: Let p_G be a *circular symmetric Gaussian* probability density on \mathbb{C}^n and let $p \neq p_G$ be any density having the same first and second moment as p_G . We denote by $H(p)$ the differential entropy of the density p , i.e. $H(p) := -\int p(a) \log p(a) da$. Then (see [16, Theorem 2]), we have the inequality

$$H(p) < H(p_G). \quad (25)$$

Now let q_G be any proper Gaussian density on \mathbb{C}^n . Under the same hypotheses, we have

$$\int \log q_G(x) p(x) dx = \int \log q_G(x) p_G(x) dx, \quad (26)$$

because $\log q_G(x)$ is a quadratic function of x . In view of (25) and (26), we now have

$$\begin{aligned} \mathbb{D}(p \| q_G) &= \int \log \frac{p(x)}{q_G(x)} p(x) dx \\ &= -H(p) - \int \log q_G(x) p(x) dx \\ &= -H(p) - \int \log q_G(x) p_G(x) dx \\ &\geq -H(p_G) - \int \log q_G(x) p_G(x) = \mathbb{D}(p_G \| q_G), \end{aligned}$$

³A proof can be worked out in the same vein of [15, Section 2].

with equality iff p_G is circular symmetric and Gaussian. Thus, if p is the solution of any minimum entropy problem with circular symmetric Gaussian prior, p has to be circular symmetric and Gaussian. ■

Lemma 4: If the second moment of p_{xv} is not finite then $\mathcal{D}(p_{xv} || p_{xy}) = \infty$.

Proof: We assume that $\mathcal{D}(p_{xv} || p_{xy})$ is finite and show that the second moment of p_{xv} is finite. Let us first recall the variational formula for the relative entropy [4, page 68]:

$$\mathcal{D}(p_{xv} || p_{xy}) = \sup_{\varphi \in \Phi} \left\{ \int_{\mathbb{C}^{2n}} \varphi(a) p_{xv}(a) da - \log \left[\int_{\mathbb{C}^{2n}} \exp[\varphi(a)] p_{xy}(a) da \right] \right\} \quad (27)$$

where Φ is the set of bounded functions. Observe now that, since p_{xy} is a Gaussian probability density, there exists $\varepsilon > 0$ such that

$$L := \mathbb{E}_{p_{xy}}[\exp[\varepsilon \|a\|^2]] = \int_{\mathbb{C}^{2n}} \exp[\varepsilon \|a\|^2] p_{xy}(a) da$$

is finite. Let us now consider the following sequence of bounded functions:

$$\varphi_l(a) := \begin{cases} \varepsilon \|a\|^2, & \text{if } \|a\|^2 \leq l, \\ 0, & \text{if } \|a\|^2 > l. \end{cases}$$

From (27) we get that for all $l = 1, 2, \dots$,

$$\mathcal{D}(p_{xv} || p_{xy}) + \log \left[\int_{\mathbb{C}^{2n}} \exp[\varphi_l(a)] p_{xy}(a) da \right] \geq \int_{\mathbb{C}^{2n}} \varphi_l(a) p_{xv}(a) da, \quad (28)$$

or, equivalently,

$$\frac{1}{\varepsilon} \left\{ \mathcal{D}(p_{xv} || p_{xy}) + \log \left[\int_{\mathbb{C}^{2n}} \exp[\varphi_l(a)] p_{xy}(a) da \right] \right\} \geq \int_{\Omega_l} \|a\|^2 p_{xv}(a) da, \quad (29)$$

where $\Omega_l := \{a \in \mathbb{C}^{2n} : \|a\|^2 \leq l\}$. As $l \rightarrow \infty$, the left-hand side of (29) converges to $\frac{1}{\varepsilon}[\mathcal{D}(p_{xv} || p_{xy}) + L]$ while the right hand side converges to the trace of the second moment of p_{xv} . Such a trace is therefore finite and thus also the second moment of p_{xv} is finite. ■

We are now ready to consider the *existence* problem. As in many optimization problems this is one of the most delicate issue.

Theorem 1: There exists an optimal solution p_{xv}^* of Problem 1.

Proof: Let d^* be the infimum of $\mathcal{D}(p_{xv} || p_{xy})$ over p_{xv} , satisfying the constraints of Problem 1. Let p_{xv}^j , $j = 1, 2, \dots$, be a sequence of probability densities satisfying the constraints of Problem 1 and such that the corresponding marginals p_{xv}^j satisfy

$$\lim_{j \rightarrow \infty} \mathcal{D}(p_{xv}^j || p_{xy}) = d^*.$$

In view of Lemma 4, we can assume that all p_{xvz}^j have finite mean vector μ_j and covariance matrix \bar{K}_j . Let m_j and K_j be the mean and covariance of $\begin{bmatrix} x \\ v \end{bmatrix}$, i.e. m_j are the first $2n$ components of μ_j and K_j is the $2n \times 2n$ upper-left block of \bar{K}_j . Now notice that, as $j \rightarrow \infty$, $\|K_j\|$ and $\|m_j\|$ remain bounded. In fact, in view of Lemma 3,

$$\mathcal{D}(p_{xv}^j || p_{xy}) \geq \mathcal{D}(p_{xv}^{Gj} || p_{xy}) = \text{trace}[K_{\begin{bmatrix} x \\ y \end{bmatrix}}^{-1} K_j] + m_j^* K_{\begin{bmatrix} x \\ y \end{bmatrix}}^{-1} m_j - \ln \left[\frac{\det[K_j]}{\det[K_{\begin{bmatrix} x \\ y \end{bmatrix}}]} \right] - 2n, \quad (30)$$

where p_{xv}^{Gj} is the Gaussian distribution having mean vector m_j and covariance matrix K_j . It is easy to check that the right-hand side of (30) diverges if at least one of $\|K_j\|$ and $\|m_j\|$ does. Hence, both $\|K_j\|$ and $\|m_j\|$ remain bounded. Thus, also μ_j and \bar{K}_j remain bounded. Therefore, there exists a subsequence $p_{xvz}^{j_i}$ such that \bar{K}_{j_i} and μ_{j_i} converge. Let \bar{K}^* and μ^* be their limits and let K^* and m^* be the limits of K_{j_i} and m_{j_i} . Notice now that each density of the corresponding sequence $p_{xvz}^{Gj_i}$ satisfies the constraints of Problem 1. In fact, the marginal p_{xz} does not change and, in view of (24), the second constraint only depends on the variance matrix. Therefore, also the Gaussian distribution p_{xvz}^{G*} , whose mean and variance are \bar{K}^* and μ^* , satisfies the constraints of Problem 1. Let p_{xv}^{G*} be the corresponding marginal. We have

$$\begin{aligned} d^* &= \lim_{i \rightarrow \infty} \mathcal{D}(p_{xv}^{j_i} || p_{xy}) \geq \lim_{i \rightarrow \infty} \mathcal{D}(p_{xv}^{Gj_i} || p_{xy}) \\ &= \lim_{i \rightarrow \infty} \text{trace}[K_{\begin{bmatrix} x \\ y \end{bmatrix}}^{-1} K_{j_i}] + m_{j_i}^* K_{\begin{bmatrix} x \\ y \end{bmatrix}}^{-1} m_{j_i} - \ln \left[\frac{\det[K_{j_i}]}{\det[K_{\begin{bmatrix} x \\ y \end{bmatrix}}]} \right] - 2n \\ &= \text{trace}[K_{\begin{bmatrix} x \\ y \end{bmatrix}}^{-1} K^*] + (m^*)^* K_{\begin{bmatrix} x \\ y \end{bmatrix}}^{-1} m^* - \ln \left[\frac{\det[K^*]}{\det[K_{\begin{bmatrix} x \\ y \end{bmatrix}}]} \right] - 2n \\ &= \mathcal{D}(p_{xv}^{G*} || p_{xy}). \end{aligned} \quad (31)$$

Thus p_{xvz}^{G*} solves Problem 1. ■

Notice that from (31) it is immediate to see that the optimal solution not only exists but is Gaussian distributed with zero mean.

Corollary 1: Let x and y be jointly Gaussian. Then the solution of Problem 1 is zero mean and Gaussian.

We are now ready to find the solution of our problem.

Theorem 2: The solution of Problem 1 is the zero mean circular symmetric Gaussian density p_{xvz}^* whose covariance matrix is

$$K_{\begin{bmatrix} x \\ v \\ z \end{bmatrix}}(Z, C) = \begin{bmatrix} K_{xx} & K_{xz}K_{zz}^{-1}Z^* & K_{xz} \\ ZK_{zz}^{-1}K_{xz}^* & ZK_{zz}^{-1}Z^* + CC^* & Z \\ K_{xz}^* & Z^* & K_{zz} \end{bmatrix}, \quad (32)$$

where Z and C solve

$$\begin{cases} C^* = C^*(ZK_{zz}^{-1}BK_{zz}^{-1}Z^* + CC^*)^{-1}A \\ Z^* = K_{zx}K_{xx}^{-1}K_{xy} + BK_{zz}^{-1}Z^*(ZK_{zz}^{-1}BK_{zz}^{-1}Z^* + CC^*)^{-1}A \end{cases} \quad (33)$$

with

$$A := K_{yy} - K_{xy}^* K_{xx}^{-1} K_{xy}, \quad (34)$$

$$B := K_{zz} - K_{xz}^* K_{xx}^{-1} K_{xz}. \quad (35)$$

Proof: We have already shown that the optimal solution is a zero-mean Gaussian distribution having covariance matrix of the form

$$K_{\begin{bmatrix} x \\ v \\ z \end{bmatrix}} = \begin{bmatrix} K_{xx} & Y & K_{xz} \\ Y^* & X & Z \\ K_{xz}^* & Z^* & K_{zz} \end{bmatrix}, \quad (36)$$

where

$$K_{\begin{bmatrix} x \\ z \end{bmatrix}} := \begin{bmatrix} K_{xx} & K_{xz} \\ K_{xz}^* & K_{zz} \end{bmatrix} > 0$$

is given. Clearly in this way the first constraint of Problem 1 is automatically satisfied for any X, Y, Z . We now show that the second constraint is equivalent to impose

$$Y = K_{xz}K_{zz}^{-1}Z^*.$$

Indeed, in view of Lemma 2, x and v are conditional orthogonal given z , so that the inverse of K_{xvz} must exhibit the zero-block pattern (24). Based on this information, we can compute Y as a function of Z and X by employing the block-matrix inversion formula:

$$M_1 = \begin{bmatrix} A_1 & B_1 \\ C_1 & D_1 \end{bmatrix} \Rightarrow M_1^{-1} = \begin{bmatrix} (A_1 - B_1 D_1^{-1} C_1)^{-1} & -A_1^{-1} B_1 (D_1 - C_1 A_1^{-1} B_1)^{-1} \\ -D_1^{-1} C_1 (A_1 - B_1 D_1^{-1} C_1)^{-1} & (D_1 - C_1 A_1^{-1} B_1)^{-1} \end{bmatrix}. \quad (37)$$

We partition $K \begin{bmatrix} x \\ v \\ z \end{bmatrix}$ as

$$K \begin{bmatrix} x \\ v \\ z \end{bmatrix} = \begin{bmatrix} A_1 & B_1 \\ C_1 & D_1 \end{bmatrix}, \quad (38)$$

where

$$A_1 := K_{xx}, \quad B_1 := \begin{bmatrix} Y & K_{xz} \end{bmatrix}, \quad C_1 := \begin{bmatrix} Y^* \\ K_{xz}^* \end{bmatrix}, \quad D_1 := \begin{bmatrix} X & Z \\ Z^* & K_{zz} \end{bmatrix}.$$

Therefore, the block in position $(1, 2)$ of K_{xvz}^{-1} (with respect to the partition (38)) is given by

$$\begin{aligned} -A_1^{-1}B_1(D_1 - C_1A_1^{-1}B_1)^{-1} &= -K_{xx}^{-1} \begin{bmatrix} Y & K_{xz} \end{bmatrix} \left(\begin{bmatrix} X & Z \\ Z^* & K_{zz} \end{bmatrix} - \begin{bmatrix} Y^* \\ K_{xz}^* \end{bmatrix} K_{xx}^{-1} \begin{bmatrix} Y & K_{xz} \end{bmatrix} \right)^{-1} \\ &= -K_{xx}^{-1} \begin{bmatrix} Y & K_{xz} \end{bmatrix} \left(\underbrace{\begin{bmatrix} X - Y^*K_{xx}^{-1}Y & Z - Y^*K_{xx}^{-1}K_{xz} \\ Z^* - K_{zx}K_{xx}^{-1}Y & K_{zz} - K_{zx}K_{xx}^{-1}K_{xz} \end{bmatrix}}_{:=M_2} \right)^{-1}. \end{aligned}$$

In order to impose the zero-block pattern (24) to the inverse, we make the block in position $(1, 1)$ in $-A_1^{-1}B_1(D_1 - C_1A_1^{-1}B_1)^{-1}$ vanish. Note that we need to compute explicitly only the elements in the first column block of M_2^{-1} . Let

$$\begin{bmatrix} A_2 & B_2 \\ C_2 & D_2 \end{bmatrix} := \begin{bmatrix} X - Y^*K_{xx}^{-1}Y & Z - Y^*K_{xx}^{-1}K_{xz} \\ Z^* - K_{zx}K_{xx}^{-1}Y & K_{zz} - K_{zx}K_{xx}^{-1}K_{xz} \end{bmatrix} = M_2$$

Thus, in view of the matrix inversion lemma, the first column block in M_2^{-1} is given by

$$\begin{bmatrix} (A_2 - B_2D_2^{-1}C_2)^{-1} \\ -D_2^{-1}C_2(A_2 - B_2D_2^{-1}C_2)^{-1} \end{bmatrix}.$$

Therefore, orthogonality of x and v given z implies

$$\begin{aligned} 0 &= -K_{xx}^{-1} \begin{bmatrix} Y & K_{xz} \end{bmatrix} \begin{bmatrix} (A_2 - B_2D_2^{-1}C_2)^{-1} \\ -D_2^{-1}C_2(A_2 - B_2D_2^{-1}C_2)^{-1} \end{bmatrix} \\ &= -K_{xx}^{-1}Y(A_2 - B_2D_2^{-1}C_2)^{-1} + K_{xx}^{-1}K_{xz}D_2^{-1}C_2(A_2 - B_2D_2^{-1}C_2)^{-1} \\ &= Y - K_{xz}D_2^{-1}C_2, \end{aligned}$$

so that

$$\begin{aligned}
Y &= K_{xz} (K_{zz} - K_{zx} K_{xx}^{-1} K_{xz})^{-1} (Z^* - K_{zx} K_{xx}^{-1} Y) \\
&= \left[\left(I + K_{xz} (K_{zz} - K_{zx} K_{xx}^{-1} K_{xz})^{-1} K_{zx} K_{xx}^{-1} \right) \right]^{-1} K_{xz} (K_{zz} - K_{zx} K_{xx}^{-1} K_{xz})^{-1} Z^* \\
&= K_{xz} K_{zz}^{-1} Z^*.
\end{aligned}$$

In this way, we have parametrized all the matrices $K \begin{bmatrix} x \\ v \\ z \end{bmatrix}$ whose inverse has the specified structure. At this point, we could minimize the divergence $\mathbb{D}(p_{xv} \| p_{xy})$ over Z and X . This turns out to be an easy problem that can be solved in closed form. This solution, however, is not the solution⁴ of our original problem since there is yet another (hidden) constraint that we need to impose. Namely we have to impose that the matrix

$$K \begin{bmatrix} x \\ v \\ z \end{bmatrix} = \begin{bmatrix} K_{xx} & K_{xz} K_{zz}^{-1} Z^* & K_{xz} \\ (K_{xz} K_{zz}^{-1} Z^*)^* & X & Z \\ K_{xz}^* & Z^* & K_{zz} \end{bmatrix} \quad (39)$$

is a *bona fide* covariance matrix, i.e. it is positive semidefinite. Since $K \begin{bmatrix} x \\ z \end{bmatrix}$ is positive definite, this constraint is equivalent to

$$X - \begin{bmatrix} (K_{xz} K_{zz}^{-1} Z^*)^* & Z \end{bmatrix} \begin{bmatrix} K_{xx} & K_{xz} \\ K_{xz}^* & K_{zz} \end{bmatrix}^{-1} \begin{bmatrix} K_{xz} K_{zz}^{-1} Z^* \\ Z^* \end{bmatrix} \geq 0$$

which, with simple algebraic manipulations, is seen to be equivalent to

$$X - Z K_{zz}^{-1} Z^* \geq 0. \quad (40)$$

The positivity constraint is then automatically satisfied if we re-parametrize the unknown matrix X in term of a new matrix C in the form

$$X = Z K_{zz}^{-1} Z^* + C C^*. \quad (41)$$

The optimal solution can be now easily obtained by solving the following *unconstrained* optimization problem

$$\arg \min_{C, Z} \mathbb{D}(p_{xv} \| p_{xy}). \quad (42)$$

⁴Here we mention this simplified optimization problem because, as discussed later, it turns out to be very useful as the first step of an efficient numerical procedure that computes the solution of our original problem.

Since

$$K_{\begin{bmatrix} x \\ v \end{bmatrix}}(Z, C) := \begin{bmatrix} K_{xx} & K_{xz}K_{zz}^{-1}Z^* \\ Z(K_{xz}K_{zz}^{-1})^* & ZK_{zz}^{-1}Z^* + CC^* \end{bmatrix}, \quad K_{\begin{bmatrix} x \\ y \end{bmatrix}} := \begin{bmatrix} K_{xx} & K_{xy} \\ K_{xy}^* & K_{yy} \end{bmatrix}, \quad (43)$$

solving (42) is equivalent to compute

$$\arg \min_{Z, C} \left\{ -\log \det(K_{\begin{bmatrix} x \\ v \end{bmatrix}}(Z, C)K_{\begin{bmatrix} x \\ y \end{bmatrix}}^{-1}) + \text{trace } K_{\begin{bmatrix} x \\ y \end{bmatrix}}^{-1}K_{xv}K_{\begin{bmatrix} x \\ v \end{bmatrix}}(Z, C) \right\}. \quad (44)$$

We are then led to the formulation of Problem 1. Let

$$J(K_{\begin{bmatrix} x \\ v \end{bmatrix}}(Z, C)) := -\log \det(K_{\begin{bmatrix} x \\ v \end{bmatrix}}(Z, C)K_{\begin{bmatrix} x \\ y \end{bmatrix}}^{-1}) + \text{trace } K_{\begin{bmatrix} x \\ y \end{bmatrix}}^{-1}K_{\begin{bmatrix} x \\ v \end{bmatrix}}(Z, C). \quad (45)$$

Its first variation is provided by

$$\begin{aligned} & D[J(K_{xv}(Z, C)); \delta K_{xv}(Z, C)] \\ &= \text{trace} [(-K_{xv}^{-1} + K_{xy}^{-1})\delta K_{xv}] \\ &= \text{trace} \left[\underbrace{(-K_{xv}^{-1} + K_{xy}^{-1})}_{=: \Delta} \begin{bmatrix} 0 & K_{xz}K_{zz}^{-1}\delta Z^* \\ \delta Z(K_{xz}K_{zz}^{-1})^* & \delta ZK_{zz}^{-1}Z^* + ZK_{zz}^{-1}\delta Z^* + \delta CC^* + C\delta C^* \end{bmatrix} \right] \\ &= \text{trace} \left[\begin{bmatrix} \Delta_{11} & \Delta_{12} \\ \Delta_{21} & \Delta_{22} \end{bmatrix} \begin{bmatrix} 0 & K_{xz}K_{zz}^{-1}\delta Z^* \\ \delta Z(K_{xz}K_{zz}^{-1})^* & \delta ZK_{zz}^{-1}Z^* + ZK_{zz}^{-1}\delta Z^* + \delta CC^* + C\delta C^* \end{bmatrix} \right] \\ &= \text{trace} \begin{bmatrix} \Delta_{12}\delta Z(K_{xz}K_{zz}^{-1})^* & * \\ * & \Delta_{21}K_{xz}K_{zz}^{-1}\delta Z^* + \Delta_{22}[\delta ZK_{zz}^{-1}Z^* + ZK_{zz}^{-1}\delta Z^* + \delta CC^* + C\delta C^*] \end{bmatrix}. \end{aligned}$$

By the properties of the trace and the Hermitian symmetry, we get that the first variation vanishes if and only if

$$\text{trace} [((K_{xz}K_{zz}^{-1})^*\Delta_{12} + Z^*K_{zz}^{-1}\Delta_{22})\delta Z + C^*\Delta_{22}\delta C] = 0. \quad (46)$$

This holds for all $\delta Z, \delta C$ if and only if

$$\begin{cases} (K_{xz}K_{zz}^{-1})^*\Delta_{12} + K_{zz}^{-1}Z^*\Delta_{22} = 0 \\ C^*\Delta_{22} = 0 \end{cases} \quad (47)$$

The first equation in (47) can be simplified so that it reads

$$K_{xz}\Delta_{12} + Z^*\Delta_{22} = 0. \quad (48)$$

The matrix inversion lemma allows to compute an explicit expression for matrix Δ

$$\begin{aligned}\Delta_{12} &= -K_{xx}^{-1}K_{xy}(K_{yy} - K_{yx}K_{xx}^{-1}K_{xy})^{-1} + \\ &\quad K_{xx}^{-1}K_{xz}K_{zz}^{-1}Z^* [ZK_{zz}^{-1}(K_{zz} - K_{zx}K_{xx}^{-1}K_{xz})K_{zz}^{-1}Z^* + CC^*]^{-1}, \\ \Delta_{22} &= (K_{yy} - K_{yx}K_{xx}^{-1}K_{xy})^{-1} - [ZK_{zz}^{-1}(K_{zz} - K_{zx}K_{xx}^{-1}K_{xz})K_{zz}^{-1}Z^* + CC^*]^{-1}.\end{aligned}$$

Now, let $A := K_{yy} - K_{yx}K_{xx}^{-1}K_{xy}$, and $B := K_{zz} - K_{zx}K_{xx}^{-1}K_{xz}$. Then we can write

$$\begin{aligned}\Delta_{12} &= -K_{xx}^{-1}K_{xy}A^{-1} + K_{xx}^{-1}K_{xz}K_{zz}^{-1}Z^* [ZK_{zz}^{-1}BK_{zz}^{-1}Z^* + CC^*]^{-1}, \\ \Delta_{22} &= A^{-1} - (ZK_{zz}^{-1}BK_{zz}^{-1}Z^* + CC^*)^{-1}.\end{aligned}$$

Therefore, after some manipulation, we conclude that the optimum solution is provided by C, Z such that

$$\begin{cases} C^* = C^*(ZK_{zz}^{-1}BK_{zz}^{-1}Z^* + CC^*)^{-1}A \\ Z^* = K_{zx}K_{xx}^{-1}K_{xy} + BK_{zz}^{-1}Z^*(ZK_{zz}^{-1}BK_{zz}^{-1}Z^* + CC^*)^{-1}A \end{cases}. \quad (49)$$

■

In view of (11) and (14), Theorem 2 provides the tightest bound to the error region (14). Indeed, let $K_{\begin{bmatrix} x \\ v \end{bmatrix}}$ be a shorthand notation for the $2n \times 2n$ upper-left corner of (32). Then, D^* is given by

$$D^* = \mathbb{D}(p_{xv}^* || p_{xy}) = -\log \det(K_{\begin{bmatrix} x \\ v \end{bmatrix}} K_{\begin{bmatrix} x \\ y \end{bmatrix}}^{-1}) + \text{trace } K_{\begin{bmatrix} x \\ y \end{bmatrix}}^{-1} \left(K_{\begin{bmatrix} x \\ v \end{bmatrix}} - K_{\begin{bmatrix} x \\ y \end{bmatrix}} \right). \quad (50)$$

Consider the circular symmetric Gaussian density p_{xvz}^* , with zero mean and variance

$$K_{\begin{bmatrix} x \\ v \\ z \end{bmatrix}} = \begin{bmatrix} K_{xx} & K_{xz}K_{zz}^{-1}Z^* & K_{xz} \\ ZK_{zz}^{-1}K_{xz}^* & ZK_{zz}^{-1}Z^* + CC^* & Z \\ K_{xz}^* & Z^* & K_{zz} \end{bmatrix}. \quad (51)$$

Note that it is such that x and v are conditionally independent given z . Then, by marginalizing and conditioning, we can obtain an optimum attacking strategy $p_{v|z}^*(\cdot|a)$ which achieves (14). It is given by the proper Gaussian density whose mean and variance are defined by

$$\mu_{v|z} := ZK_{zz}^{-1}a \quad (52)$$

$$K_{v|z} := K_{vv} - K_{vz}K_{zz}^{-1}K_{vz}^* = CC^* \quad (53)$$

IV. EFFICIENT COMPUTATION OF THE TIGHTEST BOUND

In view of Theorem 2, in order to provide the expression of the optimal solution p_{xvz}^* , we have to compute matrices C, Z which solve the system of nonlinear matrix equations (33). This appears however to be a highly non trivial task. Thus, we propose a two stage algorithm:

- 1) **Feasible (projected) Solution.** To begin with, we deal with an optimization problem which can be considered a relaxed version of Problem 1, since no positivity constraints on the matrix $K \begin{bmatrix} x \\ v \\ z \end{bmatrix}$ are imposed. This task turns out to be much simpler to achieve. Indeed, the solution can be computed in closed form. Then, we project the solution to the relaxed problem onto the feasible set, i.e. the set of pairs (X, Z) which make $K \begin{bmatrix} x \\ v \\ z \end{bmatrix}$ positive definite.
- 2) **Iterative Algorithm.** We use the projection as a starting point for an iterative update procedure whose fixed point satisfies (33).

Next we provide some details for each phase.

Feasible Solution. Minimizing (11) with no constraints on the positivity of $K \begin{bmatrix} x \\ v \\ z \end{bmatrix}$ is equivalent to solve

Problem 2:

$$\arg \min_{X, Z} J(K \begin{bmatrix} x \\ v \end{bmatrix}(Z, X)) := \left\{ -\log \det(K \begin{bmatrix} x \\ v \end{bmatrix}(Z, X) K \begin{bmatrix} x \\ y \end{bmatrix}^{-1}) + \text{trace } K \begin{bmatrix} x \\ y \end{bmatrix}^{-1} K \begin{bmatrix} x \\ v \end{bmatrix} \right\} \quad (54)$$

where

$$K \begin{bmatrix} x \\ v \end{bmatrix}(Z, X) := \begin{bmatrix} K_{xx} & K_{xz} K_{zz}^{-1} Z^* \\ Z(K_{xz} K_{zz}^{-1})^* & X \end{bmatrix}, \quad K \begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} K_{xx} & K_{xy} \\ K_{xy}^* & K_{yy} \end{bmatrix}. \quad (55)$$

In the same vein of the proof of Theorem 2, we work out the optimality conditions that X and Z have to satisfy, based on the analysis of the first variation $D[J(K \begin{bmatrix} x \\ v \end{bmatrix}(Z, X); \delta K \begin{bmatrix} x \\ v \end{bmatrix}]$. Some easy algebraic calculations lead us to the closed form of an optimal solution (Z, X) :

$$\begin{cases} Z = K_{xy}^* K_{xx}^{-1} K_{xz} (K_{xz}^* K_{xx}^{-1} K_{xz})^\dagger K_{zz}, \\ X = K_{yy} - K_{xy}^* K_{xx}^{-\frac{1}{2}} \left[I - K_{xx}^{-\frac{1}{2}} K_{xz} (K_{xz}^* K_{xx}^{-1} K_{xz})^\dagger K_{xz}^* K_{xx}^{-\frac{1}{2}} \right] K_{xx}^{-\frac{1}{2}} K_{xy} \end{cases} \quad (56)$$

where “ \dagger ” denotes Moore-Penrose pseudo inverse.

If the obtained X and Z are such that $X - Z K_{zz}^{-1} K^* \geq 0$, the algorithm terminates. Otherwise, a pair (C, Z) is obtained as follows. Let T be a unitary matrix such that $\Sigma_T := T^*(X -$

$ZK_{zz}^{-1}K^*)T = \text{diag}(d_1, d_2, \dots, d_k, \delta_1, \delta_2, \dots, \delta_h)$, where d_i are positive and in decreasing order, and δ_i are negative or zero. Let $\Sigma'_T := \text{diag}(d_1, d_2, \dots, d_k, \varepsilon, \varepsilon, \dots, \varepsilon)$, where $\varepsilon := (d_k/100) > 0$ is a “small” parameter. Let $\Sigma' := T\Sigma'_T T^* > 0$ and C be such that $CC^* = \Sigma'$.

Iterative Algorithm. We use the pair (C, Z) as a starting point for the iterations

$$\begin{cases} C^*(k+1) = C^*(k)(Z(k)K_{zz}^{-1}BK_{zz}^{-1}Z^*(k) + C(k)C^*(k))^{-1}A, \\ Z^*(k+1) = K_{zx}K_{xx}^{-1}K_{xy} + BK_{zz}^{-1}Z^*(k)(Z(k)K_{zz}^{-1}BK_{zz}^{-1}Z^*(k) + C(k)C^*(z))^{-1}A \end{cases} \quad (57)$$

where

$$A := K_{yy} - K_{xy}^* K_{xx}^{-1} K_{xy} \quad (58)$$

$$B := K_{zz} - K_{xz}^* K_{xx}^{-1} K_{xz}. \quad (59)$$

By the the iterative process we aim at finding a fixed point for (57), which provides the solution of Problem 1. The iterative process can be stopped either after a fixed number of iterations, or when the variation of D^* over one iteration is smaller than a given percentage.

V. NUMERICAL RESULTS

A. Uncorrelated Channels

In order to assess the performance of the proposed algorithm for the computation of the tightest bound, we first consider the case where $m = n$ and the covariance matrices are identities, i.e.

$$K \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} I_n & \sigma I_n & \rho I_n \\ \sigma^* I_n & I_n & \tau I_n \\ \rho^* I_n & \tau^* I_n & I_n \end{bmatrix}$$

This scenario corresponds for example to an OFDM transmission with uncorrelated channel frequency response. Beyond being an asymptotic case widely considered in the literature, this is also a practical scenario, when a subset of subcarriers with cardinality smaller than the number of channel taps is considered, and the channel taps are independent Gaussian variables. The parameter ρ dictates the correlation between channel estimates performed by Eve and the legitimate channel.

First we assess the performance of the iterative algorithm. Fig 2 shows the values of the cost of the optimum solution D^* as a function of the number of iterations for the iterative algorithm, with $n = m = 64$, and various values of ρ . We observe that the iterative algorithm always

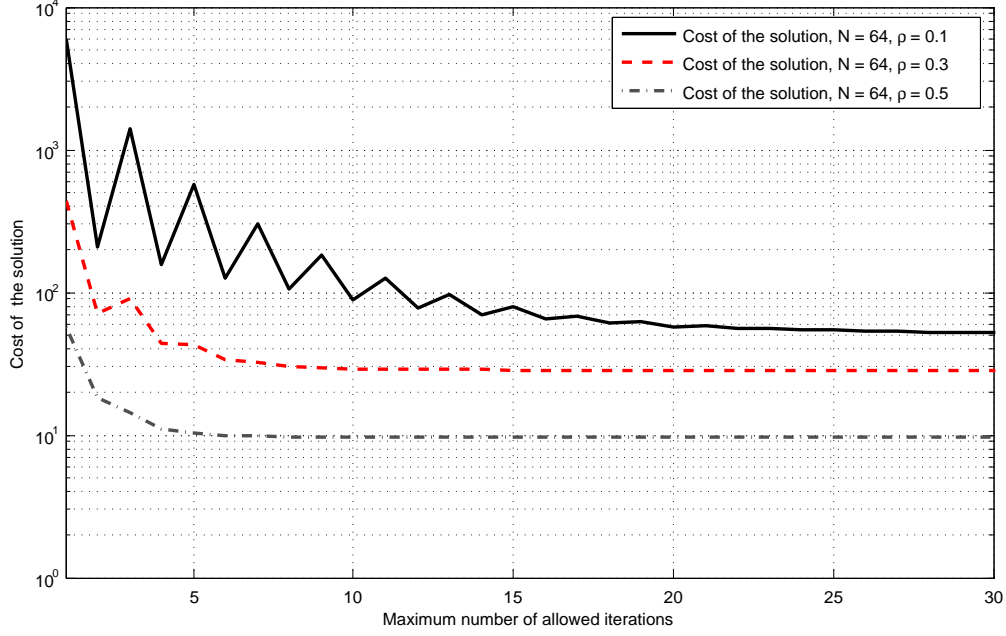


Fig. 2: Cost of the solution computed by the iterative algorithm as a function of the maximum number of iterations, with $n = m = 64$, for $\rho = 0.1, 0.3, 0.5$

converges to a fixed point for (57) and that the convergence to a solution with good accuracy takes less than 100 iterations. Thus, in the following we consider this value for the maximum number of iterations.

Fig. 3 shows the bound of the type II (β) – type I (α) error probability region for various values of the correlation parameter ρ , and for $n = m = 64$, as obtained from the proposed iterative approach. As expected, we observe that for increasing values of ρ , the region of achievable values of α and β gets wider. In particular, for the considered scenario, the type II error probability is larger than 10^{-1} already for $\rho = 0.4$.

In Fig. 4 we report the results obtained for both the initial feasible solution (projection of the solution of (56)) and final solution of the iterative algorithm, as a function of n , for $\rho = 0.1, 0.5, 0.7$. For the sake of clarity, we also show the cost of the solutions provided by the iterative algorithm in Tab. I.

We note that the iterative algorithm remarkably lowers the value of the cost function from the initial feasible solution, thus motivating its use, although it comes at a cost of more computations. Also, as expected, the cost function increases with n . For the considered case of OFDM trans-

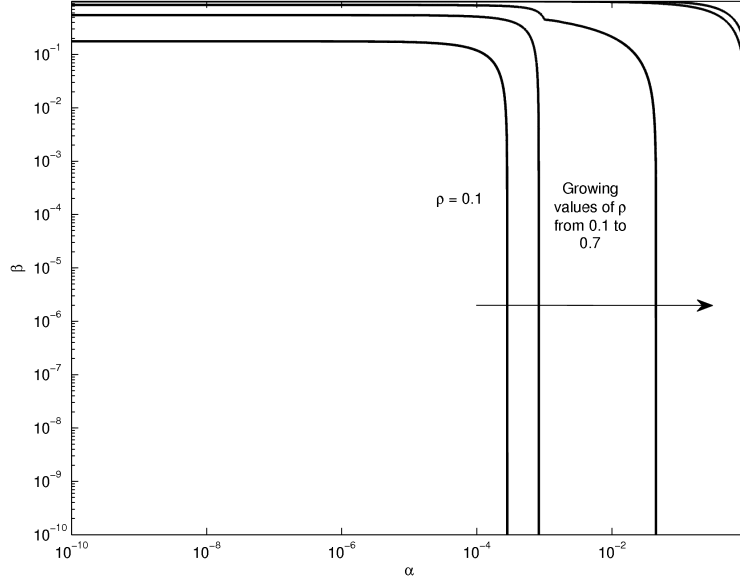


Fig. 3: Bound of the region type II (β) vs type I (α) error probability for various values of the correlation parameter ρ , with $K_{xx} = I_{n \times n}$, $K_{zz} = I_{m \times m}$, and $K_{xz} = \rho I_{n \times m}$.

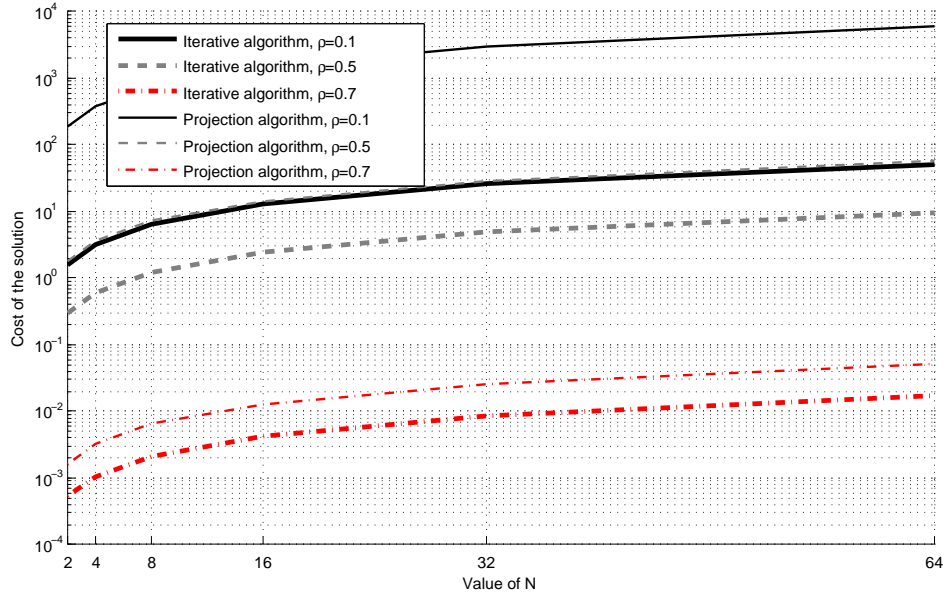


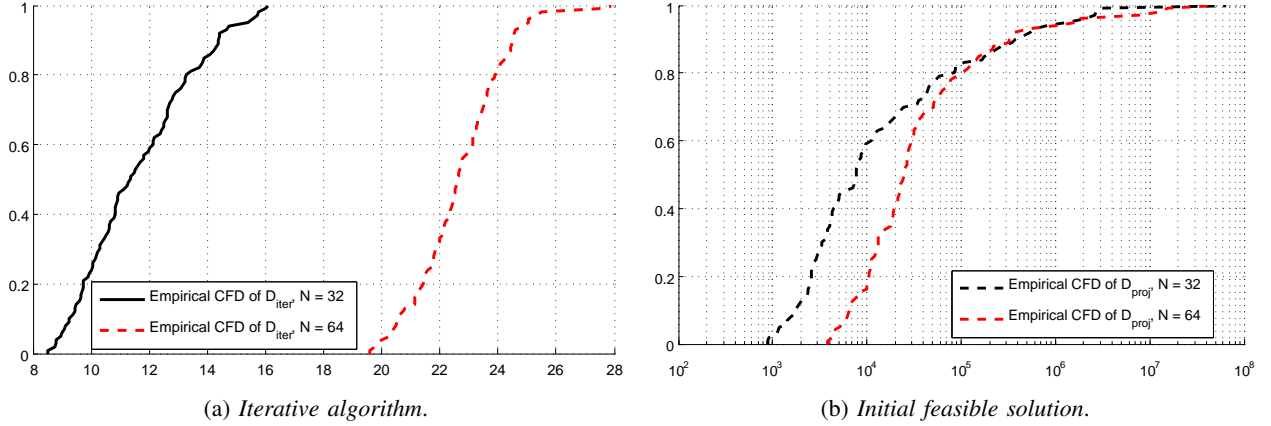
Fig. 4: Cost function D^* as a function of n for various values of the correlation parameter ρ , with $K_{xx} = I_{n \times n}$, $K_{zz} = I_{m \times m}$, and $K_{xz} = \rho I_{n \times m}$. Both projection and iterative algorithms are considered.

TABLE I: Cost of the solution provided by the iterative solution.

D^*	$n = 2$	$n = 4$	$n = 8$	$n = 16$	$n = 32$	$n = 64$
$\rho = 0.1$	1.6099	3.2199	6.4397	12.8795	25.7589	51.5179
$\rho = 0.5$	0.3047	0.6094	1.2189	2.4378	4.8756	9.7511
$\rho = 0.7$	0.0005	0.0011	0.0021	0.0042	0.0085	0.0169

mission, this means that more dispersive channels having independent taps provide potentially a better authentication system. This phenomenon has been already seen in [8].

B. Correlated Channels

Fig. 5: CDF of the cost function for two values of n .

We now consider channels with random correlation. We let $m = n$ and generate $K \begin{bmatrix} x \\ y \\ z \end{bmatrix}$ as a realization of a $3n \times 3n$ real Wishart matrix⁵. Even in this case we verified that setting the maximum number of iteration to 100 is enough for the convergence of the iterative algorithm. Fig. 5.a shows the cumulative distribution function (CDF) of D^* for two values of $n = m$, at the convergence of the iterative algorithm. Also in this case we observe that a larger n provides a

⁵A $n \times n$ real (resp., complex) *Wishart matrix* is a random matrix W that can be written as $W = AA^*$, where A is a $n \times n$ random matrix with independent identically distributed (iid) real (resp., circularly symmetric complex) Gaussian entries. In our case, the entries of A have zero mean and unit variance.

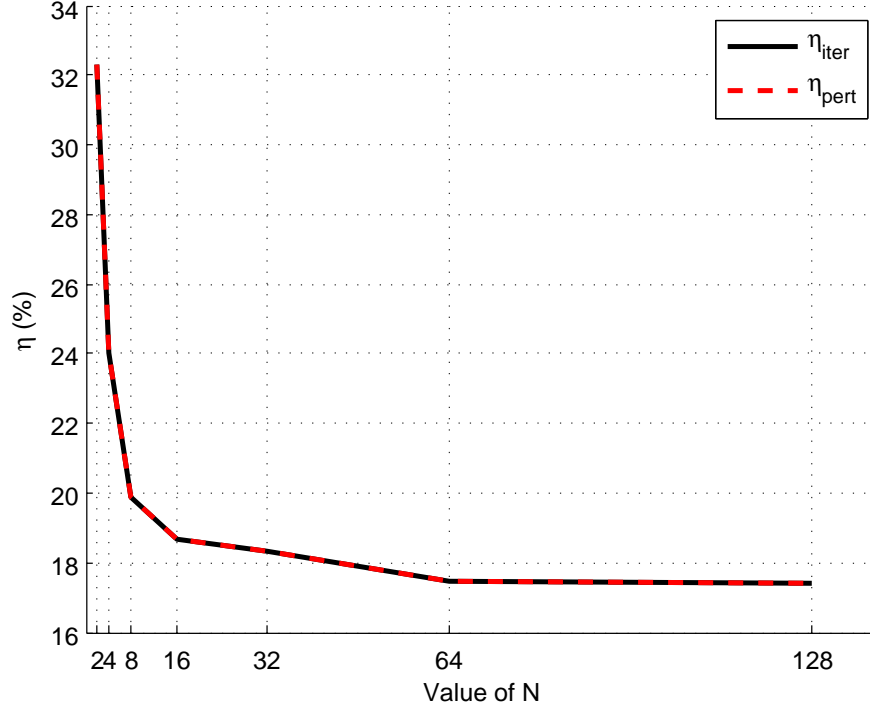


Fig. 6: Percentage improvement η as a function of n . Random correlation matrices and $n = m$. Perturbation analysis results are included.

larger value of D^* . We also report in Fig. 5.b the CDF for the initial feasible solution obtained by projection.

For the random correlation case, Tab. II shows the probability that the closed form solution of the relaxed problem (56) satisfies the positivity constraint, as a function of n .

TABLE II: Probability that (56) is feasible, as a function of n .

n	2	4	8	16	32	64
p [%]	43	10	0	0	0	0

Note that as n increases this probability goes fast to zero, thus making the projection step necessary to obtain an initial feasible solution for the iterative algorithm.

In order to compare the iterative solution to the one provided by (56), which may not fulfill the positivity constraints on the joint covariance matrix, Fig. 6 shows the percentage increase of

the cost (45) defined as

$$\eta := 100 \times \left[\frac{J_{iter}^*}{J_{cf}^*} - 1 \right], \quad (60)$$

where J_{iter}^* is the cost of the solution provided by the iterative algorithm, whereas J_{cf}^* is the cost of the one computed in closed form through (56). The analysing of the increment with regard to J^* is convenient because D_{cf}^* can vanish. Indeed, recall that, if $K_{\begin{bmatrix} x \\ y \end{bmatrix}}$ is a $n \times n$ matrix, it holds that $D^* = J^* - 2n$. We note that the increase is in the range of 20% to 30% for the considered scenario. Moreover, it is diminishing as n increases. This seems to suggest that, for growing values of n , the solution computed by means of (56) corresponds to a matrix of the form (39) which gets closer to the cone of positive definite matrices of size $(2n + m)$.

We also provide results for the perturbation analysis. In particular, we evaluate the effects of small perturbations of Z and C generated as Gaussian random variables with norm $0.01\|Z\|$ and $0.01\|C\|$, respectively. Fig. 6 reports the maximum cost function achieved for all perturbed values, showing that it provides negligible improvement with respect to the solution of the iterative approach. This supports the conclusion that the iterative approach reaches a minimum point for $\mathbb{J}(K_{\begin{bmatrix} x \\ v \end{bmatrix}}(Z, C))$. We also applied the iterative algorithm starting from the perturbed solutions which led to cost improvements. Results, not reported here, show that this procedure achieves very small improvements with an increase of the cost function of 0.01% .

VI. CONCLUSIONS

We have considered the problem of deriving a universal performance bound, for a message source authentication scheme based on channel estimates in a wireless fading scenario, where an attacker may have correlated observations available. We have formulated an outer bound to the region of achievable false alarm and missed detection probabilities, which is universal across all possible decision rules by the receiver.

Under the assumption that the channels are represented by multivariate complex Gaussian variables, we have proved that the tightest bound corresponds to a forging strategy that produces a zero mean signal that is jointly Gaussian with the attacker observations. Furthermore, we have derived a characterization of their joint covariance matrix through the solution of a system of two nonlinear matrix equations. Based upon this characterization, we have also devised an efficient iterative algorithm for its computation: The solution to the matricial system appears as fixed point of the iteration.

From numerical results, we conclude that the proposed iterative approach for the best attacking strategy always converges. Moreover, from the perturbation analysis, we deduce that the limit point is a local minimum. We have therefore provided an effective method for the attacking strategy that yields the tightest bound on the error region of the message authentication procedure.

REFERENCES

- [1] F. Carli, A. Ferrante, M. Pavon, and G. Picci. A Maximum Entropy Solution of the Covariance Extension Problem for Reciprocal Processes. *IEEE Trans. Automatic Control*. Vol. AC-56(9):1999–2012, 2011.
- [2] T. Daniels, M. Mina, and S.F. Russell, “A Signal Fingerprinting Paradigm for General Physical Layer and Sensor Network Security and Assurance,” *IEEE SECURECOMM*, pp. 1-3, Athens (Greece), Sep. 2005.
- [3] A. P. Dempster, Covariance selection, *Biometrics*, **28**,157–175, 1972.
- [4] J.-D. Deuschel, and D. W. Stroock, *Large deviations*. Academic Press, New York, 1989.
- [5] D.B. Faria and D.R. Cheriton, “Detecting identity-based attacks in wireless networks using signalprints,” *ACM WiSe*, pp. 43-52, Los Angeles (CA), Sep. 2006.
- [6] A. Ferrante and M. Pavon. Matrix Completion à la Dempster by the Principle of Parsimony. *IEEE Trans. Information Theory*. Vol. 57(6):3925–3931, 2011.
- [7] L. Xiao, L.J. Greenstein, L. Fellow, N.B. Mandayam, and W. Trappe, “Channel-based spoofing detection in frequency-selective Rayleigh channels,” *IEEE Trans. Wireless Commun.*, vol. 8, 2009, pp. 5948-5956.
- [8] P. Baracca, N. Laurenti, and S. Tomasin, “Physical layer authentication over MIMO fading wiretap channels,” *IEEE Trans. Wireless Commun.*, accepted for publication in Mar. 2012, DOI: 10.1109/TWC.2012.051512.111481
- [9] U.M. Maurer, “Authentication theory and hypothesis testing,” *IEEE Trans. Inf. Theory*, vol. 46, Jul. 2000, pp. 1350-1356.
- [10] R. E. Blahut, *Principles and Practice of Information Theory*. Reading, MA: Addison-Wesley, 1987.
- [11] C. Cachin, “An Information-Theoretic Model for Steganography,” in *International Workshop on Information Hiding, IH98*, Portland, OR, April 14-17, 1998, vol. LNCS-1525, pp. 306318.
- [12] S. Kullback, *Information Theory and Statistics*, Dover Publications, NY, 1967.
- [13] M. Barni, and B. Tondi, “The Source Identification Game: An Information-Theoretic Perspective,” *IEEE Trans. on Inform. Forens. Security*, vol. 8, no. 3, pp. 450463, Mar. 2013.
- [14] L. Lai, H. El Gamal, and H. V. Poor “Authentication Over Noisy Channels”, *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 906-916, Feb. 2009.
- [15] T. P. Speed, and H. T. Kiiveri, “Gaussian Markov Distributions over Finite Graphs”, *Annals of Statistics*, vol. 14, no. 1, pp.138-150, Mar. 1986.
- [16] F. D. Neeser, and J. L. Massey, “Proper Complex Random Processes with Applications to Information Theory”, *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp.1293-1302, Jul. 1993.